Фаріон-Мельник А.І.,
к.е.н., доцент.,доцент кафедри безпеки та правоохоронної діяльності
Західноукраїнський національний університет
Нуркович Д.
студент групи НБ-12
юридичного факультету,
Західноукраїнський національний університет

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ВИКЛИКІ ТА ПЕРСПЕКТИВИ ДЛЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

У сучасному світі цифрові технології охоплюють практично всі сфери людської діяльності, сприяючи розвитку економіки, науки та суспільства загалом. Водночас поряд із перевагами вони породжують і нові ризики, особливо у сфері безпеки. Кіберзлочинність сьогодні набуває глобального характеру, адже зловмисники активно використовують мережу Інтернет для атак на критичну інфраструктуру, фінансові установи та окремих громадян. Як визначив INTERPOL, що “кіберзлочинність не обмежується національними кордонами, що значно ускладнює діяльність правоохоронних органів та потребує міжнародної співпраці” [6, 12]. На міжнародному рівні значну роль відіграють організації, які забезпечують координацію у сфері кібербезпеки, зокрема Europol та INTERPOL.

Вони здійснюють обмін інформацією, аналітичну підтримку та сприяють міжнародному розслідуванню кіберзлочинів [5, 7]. В Україні правове регулювання у сфері кібербезпеки визначається Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, зокрема ст. 3, яка закріплює принципи державної політики у сфері кібербезпеки, та ст. 8, яка визначає повноваження

суб'єктів забезпечення кібербезпеки. Крім того, Кримінальний кодекс України передбачає відповідальність за злочини у сфері використання електронно-обчислювальних систем [2, ст. 361–363-1], які охоплюють несанкціоноване втручання в роботу комп'ютерних мереж та інші кіберзлочини.

Важливе значення має також Кримінальний процесуальний кодекс України, зокрема ст. 84, яка визначає поняття доказів, та ст. 99, де закріплено поняття електронних доказів і порядок їх використання у кримінальному провадженні [3, ст. 84, 99]. На міжнародному рівні ключовим документом є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 23.11.2001, яка встановлює основні принципи міжнародної співпраці у розслідуванні кіберзлочинів та обміні електронними доказами [4, розд. II–III]. Також у сфері захисту інформації значну роль відіграє Регламент ЄС 2016/679 (GDPR), який регулює питання захисту персональних даних.

У практичній діяльності правоохоронних органів застосовуються спеціалізовані комплекси для аналізу даних, виявлення кіберзагроз та відстеження цифрових слідів [7, 21]. Це дозволяє підвищити ефективність розслідувань та скоротити час реагування на кіберзлочини.

Отже, використання інформаційних технологій у протидії кіберзлочинності є важливим і необхідним елементом правоохоронної діяльності. Вони суттєво підвищують ефективність розслідування злочинів, дозволяють швидше виявляти кіберзагрози, аналізувати великі обсяги інформації та встановлювати зв'язки між подіями. Завдяки цьому правоохоронні органи отримують нові можливості для запобігання та розкриття правопорушень у цифровому середовищі. Водночас застосування таких технологій пов'язане з певними ризиками. Зокрема, це питання захисту персональних даних, можливість технічних

помилок у роботі алгоритмів, а також залежність від цифрових систем. Крім того, швидкий розвиток технологій часто випереджає правове регулювання, що створює додаткові виклики для держави.

Таким чином, інформаційні технології є одночасно і потужним інструментом підвищення безпеки, і джерелом нових ризиків. Саме тому їх використання повинно супроводжуватися чітким правовим регулюванням та постійним удосконаленням практики правоохоронних органів.

ЛІТЕРАТУРА:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.05.2026).
2. Кримінальний кодекс України від 05.04.2001 № 2341-III (розділ XVI, ст. 361–363-1). URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 03.05.2026).
3. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (ст. 84, 99). URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 03.05.2026).
4. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 23.11.2001. URL: https://www.coe.int (дата звернення: 03.05.2026).
5. Europol. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu (дата звернення: 03.05.2026).
6. INTERPOL. Cybercrime Reports and Cybersecurity Analysis. URL: https://www.interpol.int (дата звернення: 03.05.2026).
7. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. URL: https://www.enisa.europa.eu (дата звернення: 03.05.2026).